Colorado
Springs

Introduction to Integrated System Health Engineering and Management in Aerospace

Dr. Stephen B. Johnson
NASA Marshall Space Flight Center
sjohns22@uccs.edu

Outline of Talk

- Definitions
- Operational & Design Theory
- Principles

Integrated System Health Engineering & Management

- *ISHEM = the processes, techniques, and technologies used to design, analyze, build, verify, and operate a system to prevent faults and/or mitigate their effects*
- **Technical, individual, and social aspects**
- **Synonym: Dependable System Design and Operations**
- **“Dependability”**

Complexity

- Beyond the capability of any one person to understand or keep track of all details
  - Heterogeneous (power, propulsion, etc.)
  - Deep: requires many years of study to master
  - Scale: the system requires so many components that it is impossible for any one person to keep all in mind
  - Interactivity: interactions between internal components, and with the external environment are “messy”

Implication of Complexity

- By definition, beyond what any one person can master (our cognitive abilities are limited)
- REQUIRES communication among individuals
- Implication:
  - Engineering of a “complex” system requires excellent communication and social skills

Failure

- "A loss of intended function or performance of an unintended function."
  - Can be designer's or user's intent
- Failure is both individually and socially defined
  - "in the eye of the beholder"
  - Some "failures" are considered normal by others

Faults and Errors

- Fault: The physical or logical cause of an anomaly.
  - The "root cause", can be at various levels
  - Might or might not lead to "failure"
- Anomaly (error): A detectable undesired state.
  - The "detector" must ultimately interpret the "state" as "undesirable"
  - Can be user, designer, others

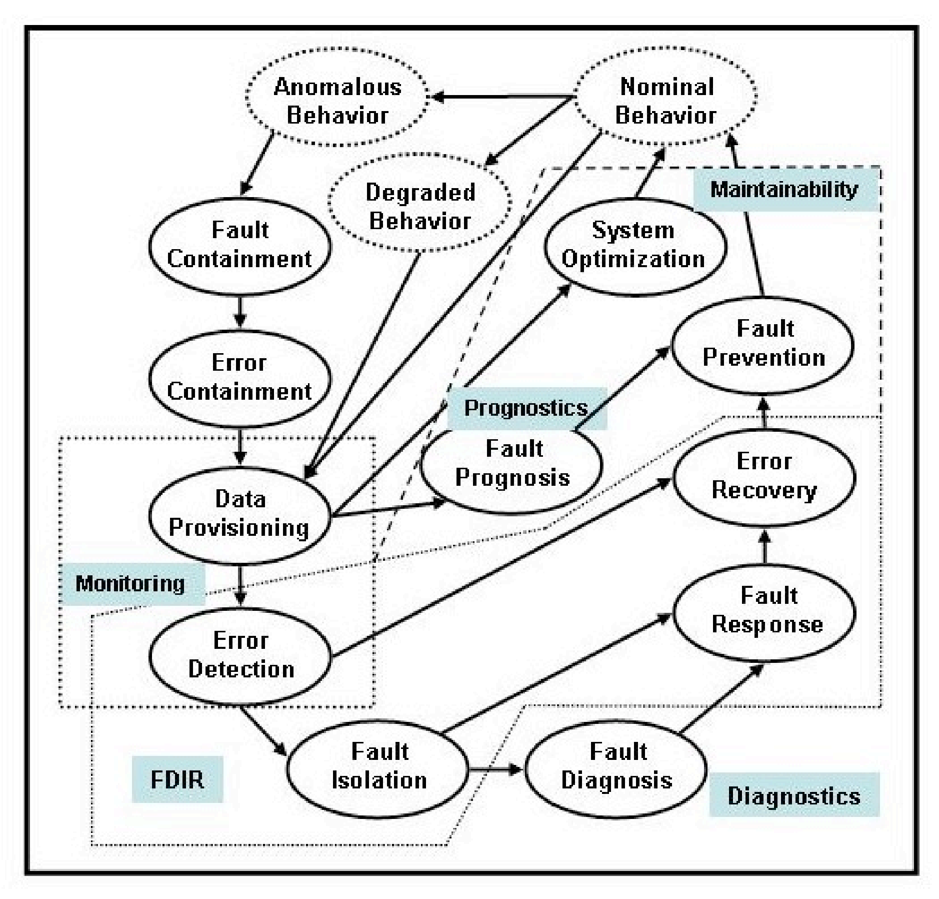
Causes of Faults and Failures

- Individual performance failure (cognitive)
  - Lack of knowledge (unaware of data)
  - Misinterpreted data
  - Simple mistakes (transposition, sign error, poor solder, etc., usually from human inattention)
- Social performance failure (communicative)
  - Miscommunication (misinterpretation)
  - Failure to communicate: information exists, but never got to the person or people who needed it

Embedded Knowledge

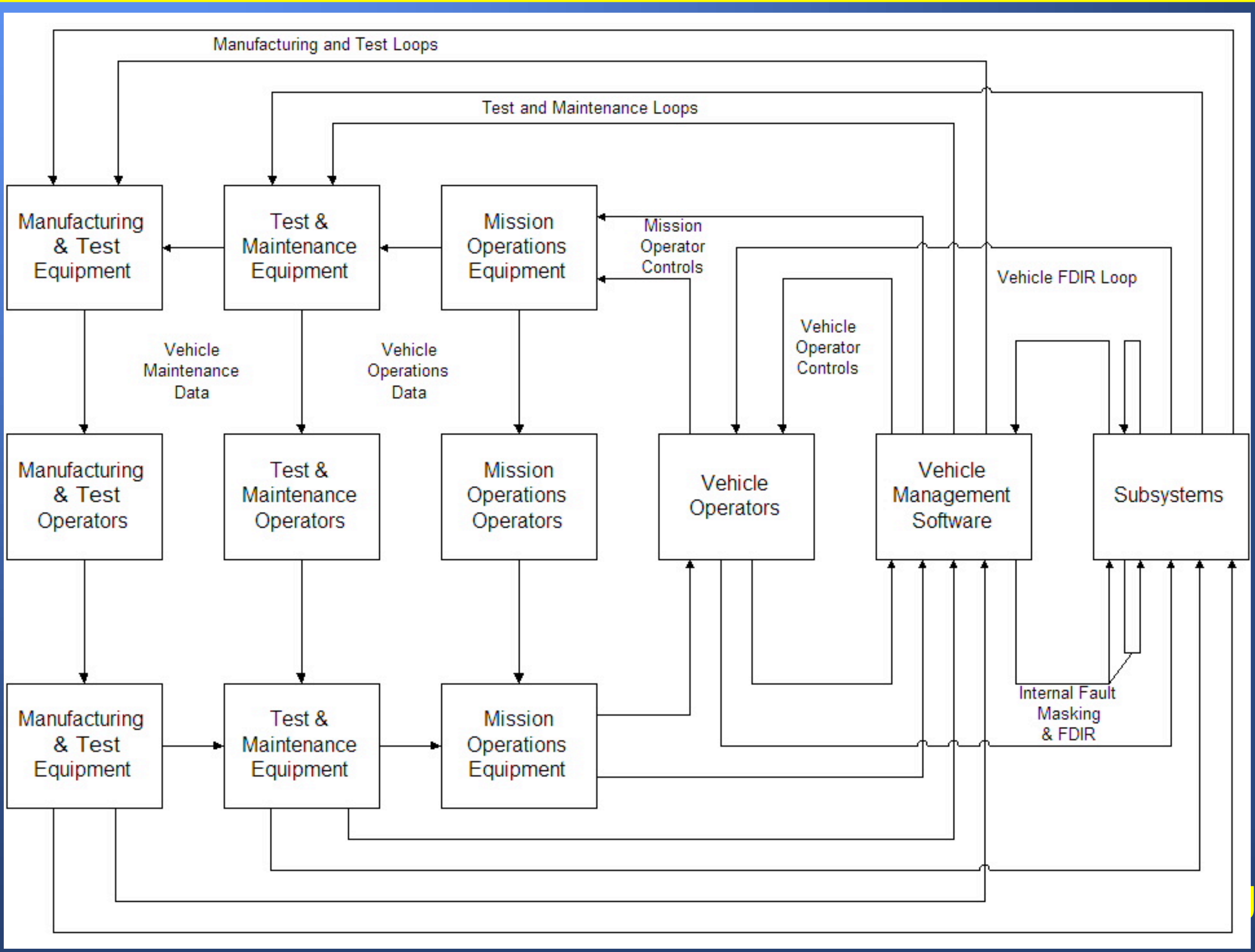
- Technologies are nothing more than “embedded knowledge”
- Technologies embody (incarnate) the knowledge of their creators
- “Faults” result from flaws in the knowledge of the creators, OR mismatch in understanding between creators and users
  - Cognitive or Communicative!

ISHEM Functional Relationships



- Circular, “closed-loop” relationships
- Hints at the physical architecture

ISHEM Operational Architecture


Manufacturing and Test Loops
Test and Maintenance Loops
Manufacturing & Test Equipment
Test & Maintenance Equipment
Mission Operations Equipment
Mission Operator Controls
Vehicle FDIR Loop
Vehicle Maintenance Data
Vehicle Operations Data
Vehicle Operator Controls
Manufacturing & Test Operators
Test & Maintenance Operators
Mission Operations Operators
Vehicle Operators
Vehicle Management Software
Subsystems
Internal Fault Masking & FDIR
Manufacturing & Test Equipment
Test & Maintenance Equipment
Mission Operations Equipment

Typical Functions, Mechanisms, and Characteristic Times

Function	Physical Mechanism	Characteristic Time
Electrical Power	Electron transport	1-10 milliseconds
Attitude Control	Thruster impulse or reaction wheel acceleration	50-500 milliseconds
Spacecraft Thermal Control	Radiative Heat Transfer	Minutes to hours
Human autonomic response	Biochemically-induced electrical signals	500 milliseconds – 1 second
Human decision-making	Verbal and visual signals between humans, and brain physiology	Minutes to days
Data computation	Electron transport and processor cycle times	10-100 milliseconds
Planetary probe radio data transfer	Electromagnetic waves	Seconds to hours

ISHEM in the System Life Cycle

	Initial Requirements	Conceptual Design	Preliminary Design	Detail Design	Fabrication and Test	Deployment & Operations
Quantitative Requirements	• Reliability Allocation • Availability • Margin Philosophy • Time to Criticality	• MTTR Req't • System TTC Timing Req'ts • Margin Allocations	• Subsystem TTC Timing Req'ts • Margin Req'ts • Reliability Req'ts	• Final Margin & Reliability Req'ts	• Requirements Updates	• Requirements Updates
Qualitative Requirements	• System FT Req'ts • System FA Req'ts • Isolation • Fault Classes for FT	• Subsystem FT Req't • Subsystem Functional Fault Req't	• Fault Injection Req'ts • SW, HW, Operations Req'ts	• Final System/ Subsystem/ Component Req'ts	• Requirements Updates	• Requirements Updates
Fault Set Definition	• Fault Classes • Major Implementation Fault Types (Engine Out, Electronics, ...)	• Subsystem Functional Faults (Top Down)	• Preliminary FMEA (Bottom Up) • Preliminary Fault Set Reduction for Fault Injection	• Final FMEA • Fault Set Reduction for Fault Injection	• Updates to Fault Set	• Updates to Fault Set
Fault Analysis & Modeling	• System Cost / Reliability Trades • Testability Analysis	• System Interaction TTC Analysis • Functional Fault Matrix • Initial Behavioral Model	• Detailed Sys. Mod. • Detailed Rel. Anal. • Simulation with Fault Injection • Cost / Reliability Anal. for Params.	• Simulation with Fault Injection • False Alarm Analysis	• Fault Injection into As Built System • System Characterization • Model Updates	• System Characterization • Model Updates • Fault and Contingency Analyses
System Design	• Initial System Concept • Operations and Maintenance Concepts	• Initial Subsystem Concept • ECR/FCR Definition at Function Level	• Detail ECR/FCR • Parameter, Algorithm, and Sensor Selection	• Final Design • Threshold Determination	• Design Feedback • Threshold Adjustment from System Characterization	• System Characterization • Design Updates • Contingency Plans
Verification & Validation	____	• V&V Plan Draft for SHM • Allocation of V&V Methods: Test, Analysis, Proof, Simulation	• Incorporate Prelim FMEA into V&V • Define Fault Inject Techniques • Proof of Key Algorithms	• Test Procedures • V&V by Analysis, Simulation, Test, and Formal Proof	• Subsystem and System Testing Under Stressing Conditions & Fault Conditions	• Testing Updates

Principle of Knowledge Redundancy, and Limits

- Checking for failure or faults requires a separate, independent, credible knowledge source
- Commonality means that reviewers share common assumptions with the reviewed
- Independence means reviewers share nothing in common with the reviewed
- Complete independence neither possible nor desirable

Clean Interfaces

- Desired and sometimes required
- Reduce the “interactivity” between components
- Reduce the interactivity of the people and organizations designing and operating the components
- Simplifies communication, reduces chance for miscommunication!

Bureaucracy and “Situational Awareness”

- Bureaucracy needed to institute and repeat processes for dependability
- Bureaucratization: repetition and suppression or forgetting of reasons behind the rules leads to inattention or misunderstanding, and hence to faults
- Must foster individual “awareness” within the bureaucracy… create bureaucracy to fight the deadening effect of bureaucracy!

Conclusion

- NASA has a “culture problem” that leads to occasional failures
- The problem is social and cognitive as well as technical
- ISHEM to be the overarching theory over the technical, social, and cognitive aspects of preventing & mitigating failure
- We are working to install / instill ISHEM into the new Vision for Space Exploration